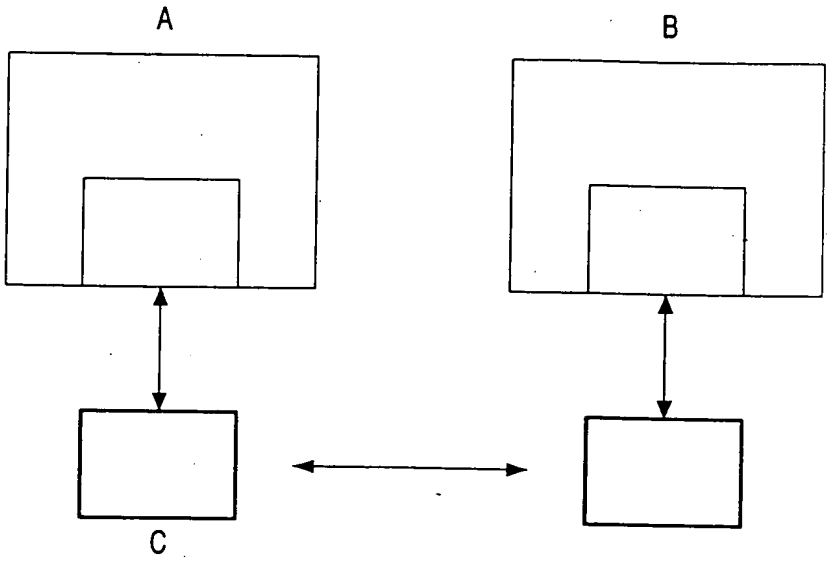
A
B
C

FIG. 1

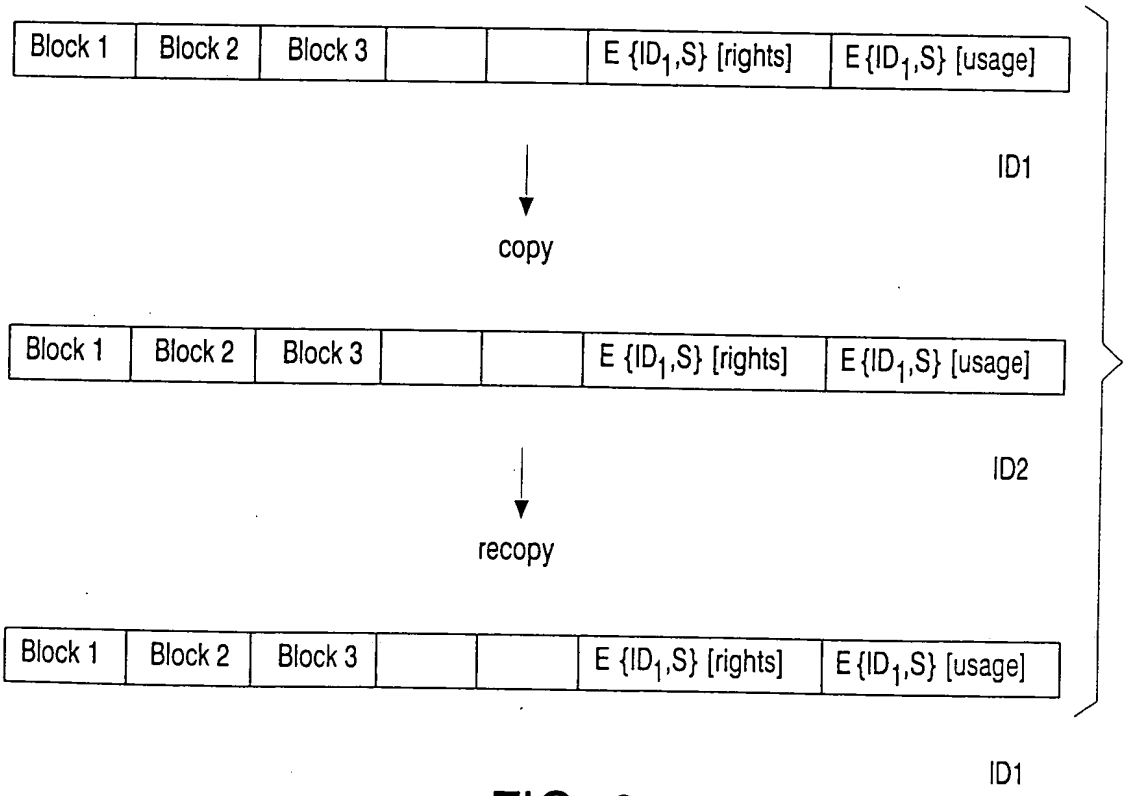
Block 1
Block 2
Block 3
E {ID1,S} [rights]
E {ID1,S} [usage]
ID1
copy
Block 1
Block 2
Block 3
E {ID1,S} [rights]
E {ID1,S} [usage]
ID2
recopy
Block 1
Block 2
Block 3
E {ID1,S} [rights]
E {ID1,S} [usage]
ID1

FIG. 2

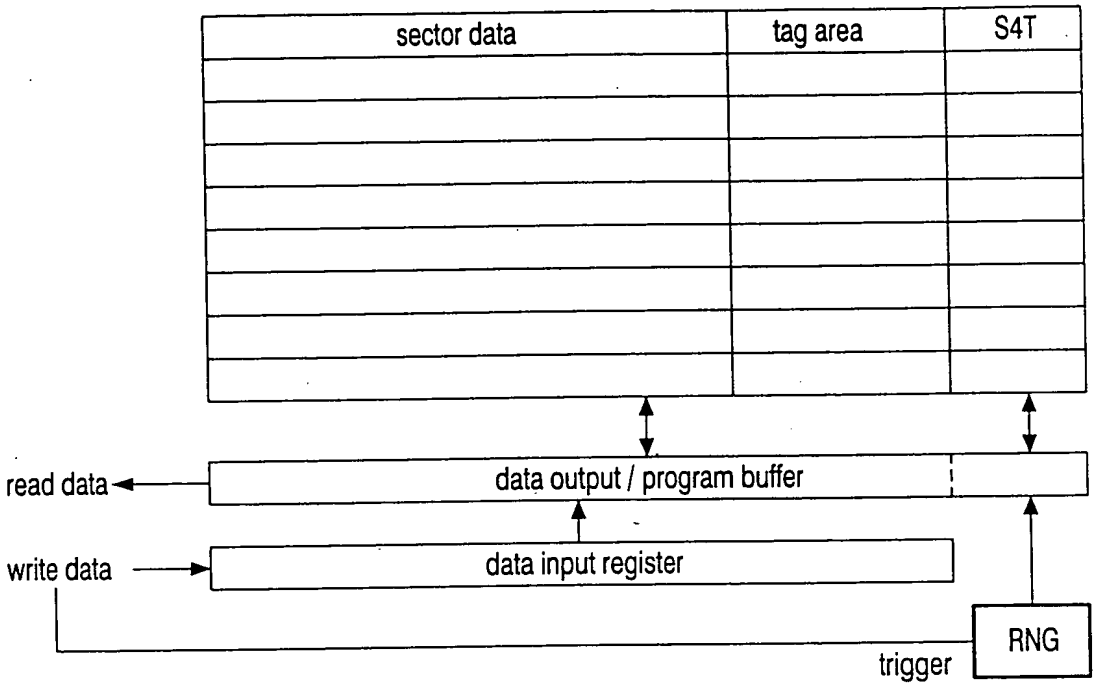

FIG. 3

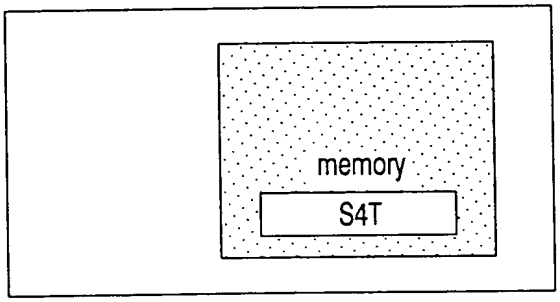

FIG. 4a

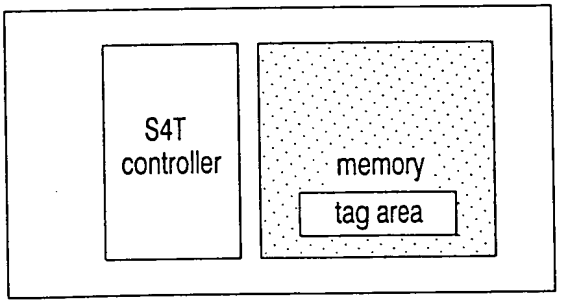

FIG. 4b

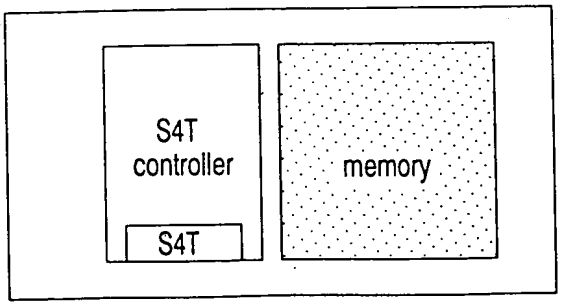

FIG. 4c

09/700383 - 11/09/00

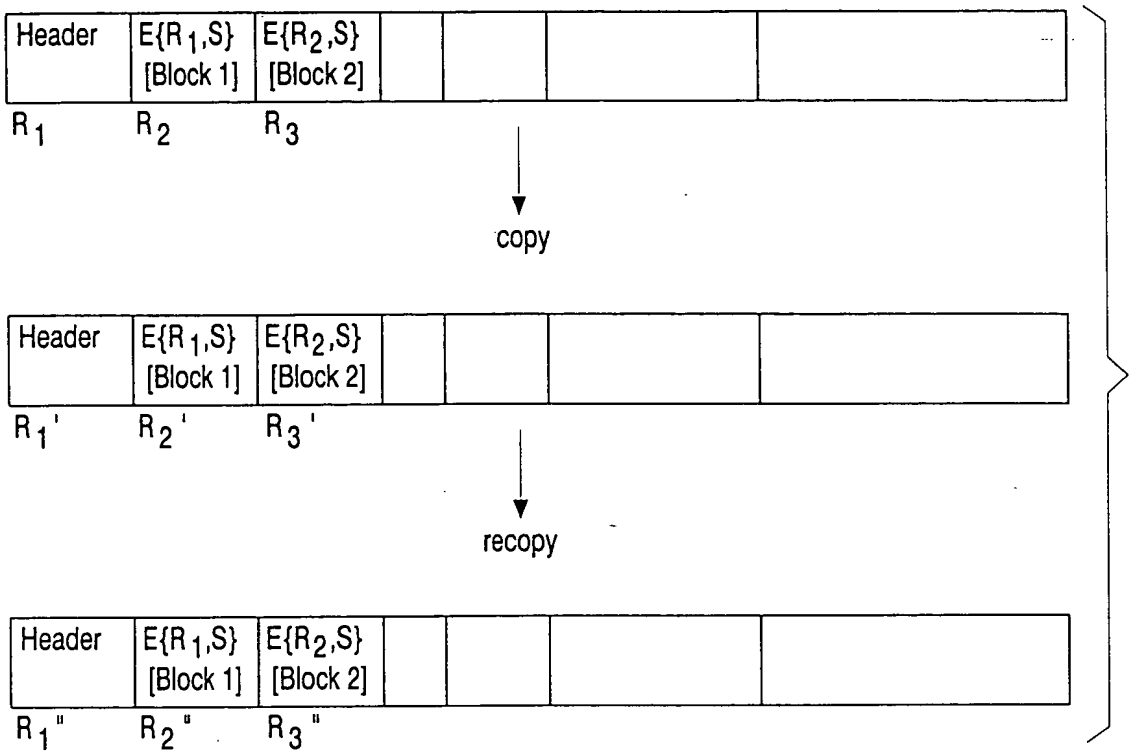
Header
E{R1,S} [Block 1]
E{R2,S} [Block 2]
R1
R2
R3
copy
Header
E{R1,S} [Block 1]
E{R2,S} [Block 2]
R1'
R2'
R3'
recopy
Header
E{R1,S} [Block 1]
E{R2,S} [Block 2]
R1"
R2"
R3"

FIG. 5

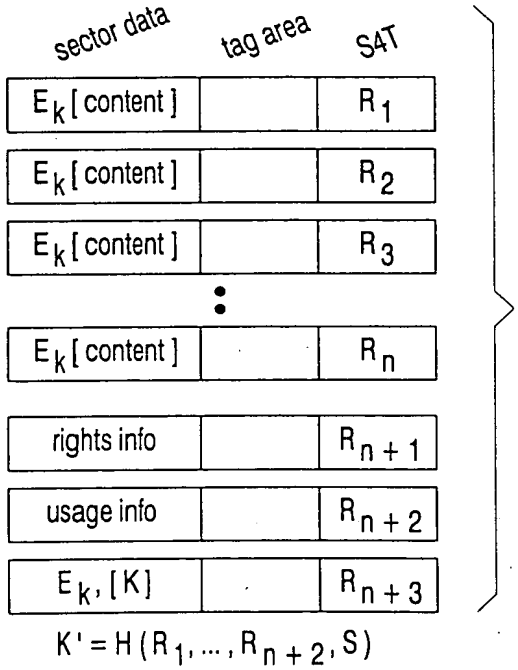
sector data
tag area
S4T
Ek[content]
R1
Ek[content]
R2
Ek[content]
R3
Ek[content]
Rn
rights info
Rn+1
usage info
Rn+2
Ek'[K]
Rn+3
K' = H(R1, ..., Rn+2, S)

FIG. 6a

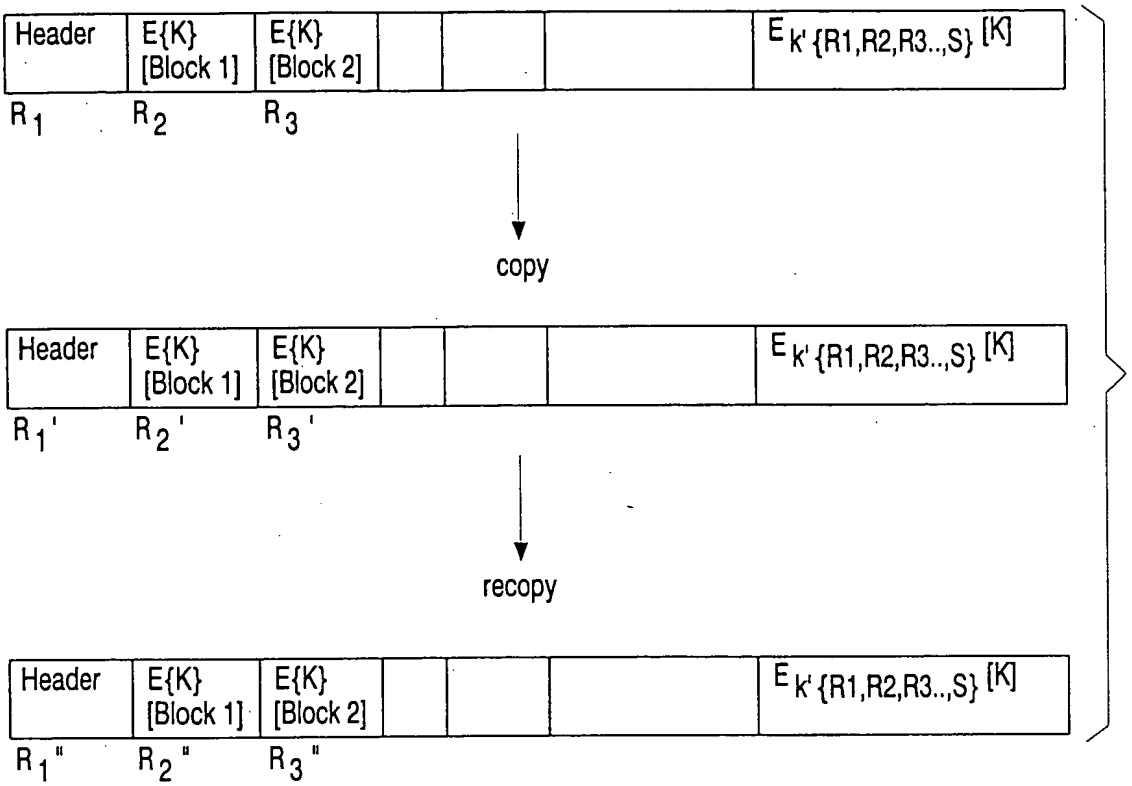

FIG. 6b

Sector data	S4T
ID_A, Enc [$K_{Pub,A}$; S, ID_A, x, y]	T_1
ID_A, Enc [$K_{Priv,A}$; H [T_1, S, ID_A, x, y]]	T_2
E [K; audio]	T_J
...	...
E [K; audio]	T_N
rights info	T_{N+1}
usage info	T_{N+2}
Enc [H [T_J, ..., T_N, T_{N+1}, T_{N+2}, S]; K]	...

FIG. 7

Sector data	S4T
ID_A, Enc [$K_{Pub,A}$; S, ID_A, x, y]	T_1
ID_A, Enc [$K_{Priv,A}$; H [T_1, S, ID_A, x, y]]	T_2
ID_B, Cert ($K_{Pub,B}$)	...
E [K; audio]	T_J
...	...
E [K; audio]	T_N
rights info	T_{N+1}
usage info	T_{N+2}
Enc [H [T_J, ..., T_N, T_{N+1}, T_{N+2}, S]; K]	...

FIG. 8

Sector data	S4T
ID_A, Enc [$K_{Pub,A}$; S, ID_A, x, y]	T_1
ID_A, Enc [$K_{Priv,A}$; H [T_1, S, ID_A, x, y]]	T_2
ID_B, Enc [$K_{Pub,B}$, S, ID_A, T_1, T_2]	T_3
E [K; audio]	T_J
...	...
E [K; audio]	T_N
rights info	T_{N+1}
usage info	T_{N+2}
Enc [H [T_J, ..., T_N, T_{N+1}, T_{N+2}, S]; K]	...

FIG. 9

Sector data	S4T
ID_A, Enc [$K_{Pub, A}$; S, ID_A, x, y]	T_1
ID_A, Enc [$K_{Priv, A}$; H [T_1, S, ID_A, x, y]]	T_2
ID_B, Enc [$K_{Pub, B}$; S, ID_B, p, q]	T_3
ID_B, Enc [$K_{Priv, B}$; H [T_3, S, ID_B, p, q]]	T_4
E [K; audio]	T_J
...	...
E [K; audio]	T_N
rights info	T_{N+1}
usage info	T_{N+2}
Enc [H [T_J, ..., T_N, T_{N+1}, T_{N+2}, S]; K]	...

FIG. 10

Sector data	S4T
ID_A, Enc [$K_{Pub, A}$; S, ID_A, x, y]	T_1
ID_A, Enc [$K_{Priv, LMC}$; H [T_1, S, ID_A, x, y]]	T_2
ID_B, Enc [$K_{Pub, B}$; S, ID_B, p, q]	T_3
ID_B, Enc [$K_{Priv, LMC}$; H [T_3, S, ID_B, p, q]]	T_4
ID_{LMC} Cert ($K_{Pub, LMC}$)	...
E [K; audio]	T_J
...	...
E [K; audio]	T_N
rights info	T_{N+1}
usage info	T_{N+2}
Enc [H [T_J, ..., T_N, T_{N+1}, T_{N+2}, S]; K]	...

FIG. 11